USDA VULNERABILITY CHECKLIST FOR TELECOMMUNICATIONS SYSTEMS

August 3, 2001

Prepared for:

United States Department of Agriculture

Office of the Chief Information Officer (OCIO)

Prepared by:

Booz·Allen & Hamilton, Inc.
3190 Fairview Park Drive
Falls Church, VA 22042

USDA Vulnerability Checklist for Telecommunications Systems

TABLE OF CONTENTS

1. INTRODUCTION

Protection of information assets and maintaining the availability, integrity, and confidentiality of USDA information technology systems and telecommunications resources are vital in meeting USDA's program delivery requirements. Information security has emerged as a top priority for the Department of Agriculture. As technology has enhanced the ability to share information instantaneously between computers and networks, it has also made USDA organizations more vulnerable to a wider variety of threats including unlawful and destructive penetration and disruptions.

USDA's mandate for securing its information systems arises from the Computer Security Act of 1987. This law and guidance from the Office of Management and Budget provide the Department with the basic security requirements. In addition, on May 22, 1998, Presidential Decision Directive 63 (PDD 63), explaining key elements of the White House's policy on critical infrastructure protection, was released. It calls for a national effort to assure the security of the United States' increasingly vulnerable and interconnected infrastructure, particularly its cyber systems. These requirements, along with his own concerns, have led the Secretary to direct the Office of the Chief Information Officer (OCIO) to develop a strategy to improve USDA's cyber security. A key aspect of this strategy is the implementation of an information systems risk management program. In particular USDA must implement a structured approach to assess risks to USDA information assets and identify vulnerabilities.

1.1 PURPOSE

This Vulnerability Checklist is designed to assist Agency ISSPMs in satisfying their responsibility to develop and implement a comprehensive risk management program as defined in DR 3140-001, "USDA Information Systems Security Policy." By using this guide, Agency ISSPMs can identify areas where Department Information Security requirements are not being met and develop an action plan to ensure all security requirements are satisfied.

1.2 SCOPE

This guide is to be used by all USDA organizational elements to help assess the security posture of various USDA telecommunications systems.

1.3 ORGANIZATION

This document is organized from the general to the specific. Common configuration management between all telecommunication equipment is address in the first section followed by the common physical security requirements. Specific Telecommunications devices are then addressed in more detail pertaining to their unique configurations. The telecommunications equipment selected covers a wide variety of the USDA network infrastructure and should provide a good basis to assess the overall telecommunications network security posture.

2. VULNERABILITY CHECKLIST

Three answers are possible when completing the checklist:

- Yes Requirement is met
- No Requirement is not met
- Other In progress, planned, or not applicable (N/A)

When using this checklist, a "yes" answer means the current configuration addresses the vulnerability in question. A "no" answer means that the vulnerability is not directly addressed but may be mitigated by other circumstances (these can be explained in the "Remarks" section. No telecommunication equipment is likely to have all "yes" answers and all equipment will assume a certain level of risk in order to be usable. N/A means that the question is not applicable to a particular device. Again, additional details if required can be added to the remarks section.

The following key should be used to identify the applicable source for each requirement.

Source Key *	
Administrative/Management Security Requirements	USDA A/MSR
Physical Security Requirements	USDA PHYSR
Personnel Security Requirements	USDA PERSR
Information Security Requirements	USDA ISR
Communications Security Requirements	USDA COMMSR
Computer Security Requirements	USDA COMPTSR
Industry Best Practices	BEST PRACTICES

2.1 GENERAL SECURITY ITEMS

2.1.1 Configuration Management

GENERAL					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	All USDA agencies and offices shall be in compliance with USDA configuration management policies and practices.	BEST PRACTICES			
2.1.1.1	Does an organizational telecommunications configuration management plan exist?				
Remarks:					
2.1.1.2	Are changes to the organizational telecommunications configuration controlled and approved by a configuration control board (CCB)?				
Remarks:					
2.1.1.3	Is a security administrator assigned to the CCB as a permanent member of the CCB?				
Remarks:					
2.1.1.4	Does the configuration management process include all hardware, software and documentation (diagrams, inventory, cable management) to support ongoing configuration status accounting and configuration audits?				
Remarks:					
2.1.1.5	Does the organization have a baseline telecommunications configuration in place?				
Remarks:					
2.1.1.6	Does management review, approve and document changes recommended by the CCB prior to moving those changes into production?				
Remarks:					

2.1.2 Telecommunication Security Policy

POLICY AND GUIDELINES					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	All USDA agencies and offices shall be in compliance with USDA security policies.	USDA A/MSR 1, 2, 4 & 97;			
2.1.2.1	Does the agency have a telecommunications security policy?				
Remarks:					

2.1.2.2	Does the agency have a telecommunications security plan?				
Remarks:					
2.1.2.3	Is the agency telecommunications security policy reviewed and revised to reflect technology changes?				
Remarks:					
2.1.2.4	Does the telecommunications security policy conform to USDA's communications guidelines and policies?				
Remarks:					
2.1.2.5	Does a policy exist to report unauthorized activity?				
Remarks:					
2.1.2.6	Does a policy exist for "appropriate" personal use of company equipment?				
Remarks:					
	A completed risk analysis shall accompany all requests for exceptions on existing dial-up circuits accessing sensitive AIS or networks.	USDA A/MSR 8 & 35 - 40			
2.1.2.7	Does a documented process exist to conduct periodic risk analysis to assess threats and vulnerabilities of telecommunication systems?				
Remarks:					
2.1.2.8	Does a documented process exist to conduct a risk analysis to assess threats and vulnerabilities prior to the installation of new equipment and/or software for telecommunication systems?				
Remarks:					
2.1.2.9	Does a documented process exist to conduct a risk analysis to assess threats and vulnerabilities prior to significant changes to and upgrades of the existing telecommunication systems?				
	For Routers?				
	For Switches?				
	For Firewalls?				
	For IDS?				
	For RAS Systems?				
	For PBX Systems?				
Remarks:					

	The certification shall determine the extent to which a particular design and implementation meets a specified set of security requirements.	USDA A/MSR 43 - 52			
2.1.2.10	Has a security survey of the telecommunication system been conducted for certification purposes?				
Remarks:					
2.1.2.11	Have the sensitive telecommunication systems been accredited, if accreditation is needed?				
Remarks:					
	A formal memorandum of understanding (MOU) among external agencies accrediting authorities preceding telecommunication interconnections of accredited applied information systems (AIS) will exist.	USDA A/MSR 11			
2.1.2.12	Does a formal memorandum of understanding (MOU) between USDA and external agencies with telecommunication interconnections exist?				
Remarks:					
	A security awareness and training program shall be established.	USDA A/MSR 75 - 78			
2.1.2.13	Is security awareness and training provided to administrators and users within the organization?				
Remarks:					
2.1.2.14	Is there a system to verify that administrators and users have taken security awareness and training?				
Remarks:					
	Data files should be backed up frequently and stored off-site or in a secured environment.	USDA COMPTSR 41			
2.1.2.15	Does an archiving policy, for the log files exist?				
	For Routers?				
	For Switches?				
	For Firewalls?				
	For IDS?				
	For RAS Systems?				
	For PBX Systems?				
Remarks:					

2.1.3 Logging & Auditing

LOGGING & AUDITING					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	Telecommunication networks shall be protected with devices or techniques that provide auditing.	BEST PRACTICES			
2.1.3.1	Do the audit logs record alarms, successful and unsuccessful log on and log off events?				
	For Routers?				
	For Switches?				
	For Firewalls?				
	For IDS?				
	For RAS Systems?				
	For PBX Systems?				
Remarks:					
2.1.3.2	Do the audit logs record that date and time of events?				
	For Routers?				
	For Switches?				
	For Firewalls?				
	For IDS?				
	For RAS Systems?				
	For PBX Systems?				
Remarks:					
2.1.3.3	Do the audit logs record user or entity identification associated with events?				
	For Routers?				
	For Switches?				
	For Firewalls?				
	For IDS?				
	For RAS Systems?				
	For PBX Systems?				
Remarks:					

2.1.3.4	Do the audit logs record the origin of events?			
	For Routers?			
	For Switches?			
	For Firewalls?			
	For IDS?			
	For RAS Systems?			
	For PBX Systems?			
Remarks:				
2.1.3.5	Do the audit logs record the type of event?			
	For Routers?			
	For Switches?			
	For Firewalls?			
	For IDS?			
	For RAS Systems?			
	For PBX Systems?			
Remarks:				
2.1.3.6	Do the audit logs record the success or failure of administrative events?			
	For Routers?			
	For Switches?			
	For Firewalls?			
	For IDS?			
	For RAS Systems?			
	For PBX Systems?			
Remarks:				
2.1.3.7	Do system administrators review audit logs weekly?			
Remarks:				

	The audit data shall be protected by the system so that "read" access to it is limited to those who have business needs for audit data.	USDA COMPTSR 35			
2.1.3.8	Are the log files only accessible to authenticated users?				
	For Routers?				
	For Switches?				
	For Firewalls?				
	For IDS?				
	For RAS Systems?				
	For PBX Systems?				
Remarks:					
	"Hashing" the log files provides authentic forensic evidence.	BEST PRACTICES			
2.1.3.9	Are the log files "hashed" to maintain authenticity?				
	For Routers?				
	For Switches?				
	For Firewalls?				
	For IDS?				
	For RAS Systems?				
	For PBX Systems?				
Remarks:					

2.1.4 Passwords

PASSWORDS					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	Strong password management is required.	USDA COMPTSR 11 – 17 & 19 - 24			
2.1.4.1	Have default passwords for maintenance accounts and software packages been changed?				
	For Routers?				
	For Switches?				
	For Firewalls?				
	For IDS?				
	For RAS Systems?				
	For PBX Systems?				

Remarks:				
2.1.4.2	Does the telecommunications system suppress or block out the clear-text representation of the password on the data entry device?			
	For Routers?			
	For Switches?			
	For Firewalls?			
	For IDS?			
	For RAS Systems?			
	For PBX Systems?			
Remarks:				
2.1.4.3	Does the telecommunications system block the demonstration of the password length?			
	For Routers?			
	For Switches?			
	For Firewalls?			
	For IDS?			
	For RAS Systems?			
	For PBX Systems?			
Remarks:				
2.1.4.4	Are null passwords disallowed?			
	For Routers?			
	For Switches?			
	For Firewalls?			
	For IDS?			
	For RAS Systems?			
	For PBX Systems?			
Remarks:				

2.1.4.5	Does the telecommunication system enforce password aging (e.g. every 60 days)?			
	For Routers?			
	For Switches?			
	For Firewalls?			
	For IDS?			
	For RAS Systems?			
	For PBX Systems?			
Remarks:				
2.1.4.6	Does the system restrict users from reusing passwords?			
	For Routers?			
	For Switches?			
	For Firewalls?			
	For IDS?			
	For RAS Systems?			
	For PBX Systems?			
Remarks:				
2.1.4.7	Does the telecommunications system ensure complex passwords (e.g. minimum length, password composition)?			
	For Routers?			
	For Switches?			
	For Firewalls?			
	For IDS?			
	For RAS Systems?			
	For PBX Systems?			
Remarks:				

	Passwords and user IDs should be immediately removed when an authorized user no longer needs access to the system.	USDA COMPTSR 18			
2.1.4.8	Is there a documented process to ensure user IDs and passwords are controlled when a user no longer needs access to the system?				
	For Routers?				
	For Switches?				
	For Firewalls?				
	For IDS?				
	For RAS Systems?				
	For PBX Systems?				
Remarks:					

2.1.5 Integrity

INTEGRITY					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	Systems and files should be scanned for vulnerabilities.	BEST PRACTICES			
2.1.5.1	Are the telecommunication systems scanned for vulnerabilities?				
	For Routers?				
	For Switches?				
	For Firewalls?				
	For IDS?				
	For RAS Systems?				
	For PBX Systems?				
Remarks:					
2.1.5.2	Are vulnerability tools updated on a weekly or bi-weekly basis (or, when new signatures are released)?				
	For Routers?				
	For Switches?				
	For Firewalls?				
	For IDS?				
	For RAS Systems?				
	For PBX Systems?				
Remarks:					

	Organizational responsibility for security is defined.	BEST PRACTICES			
2.1.5.3	Is there a dedicated security administrator?				
Remarks:					
2.1.5.4	Is there an individual who can serve as a backup to the dedicated security administrator?				
Remarks:					
2.1.5.5	Are all security functions and software changes made only by authorized administrators?				
Remarks:					

2.1.6 Service Continuity

SERVICE CONTINUITY					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	Disaster recovery and continuity of operations for all information technology installations shall be maintained.	USDA A/MSR 67 - 68 & 74			
2.1.6.1	Does a contingency plan exist for telecommunication systems?				
Remarks:					
2.1.6.2	Has the contingency plan been tested?				
Remarks:					
	Systems should be backed up on a regular basis.	USDA COMPTSR 41			
2.1.6.3	Are the telecommunication systems backed up if possible?				
	For Routers?				
	For Switches?				
	For Firewalls?				
	For IDS?				
	For RAS Systems?				
	For PBX Systems?				
Remarks:					

2.1.6.4	Is the backup media stored at an off-site facility?				
	For Routers?				
	For Switches?				
	For Firewalls?				
	For IDS?				
	For RAS Systems?				
	For PBX Systems?				
Remarks:					
	New software should be backed up immediately, retaining the original distribution diskettes in a safe and secure location.	USDA COMPTSR 40			
2.1.6.5	Is software/media backed up immediately after installation?				
	For Routers?				
	For Switches?				
	For Firewalls?				
	For IDS?				
	For RAS Systems?				
	For PBX Systems?				
Remarks:					
2.1.6.6	Is the original software media stored in a secure location?				
	For Routers?				
	For Switches?				
	For Firewalls?				
	For IDS?				
	For RAS Systems?				
	For PBX Systems?				
Remarks:					

Period of: (Month/Year) _____ to (Month/Year) _____		
Reviewed by:	Name:	Signature:
Date Reviewed:		

2.2 PHYSICAL SECURITY

PHYSICAL SECURITY					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	Physical security for the central computer facility will be commensurate with the minimum requirements of the most restrictive category of information processed by the system.	USDA PHYSR 1			
2.2.1	Are systems located in a secured AIS room or location?				
	For Routers?				
	For Switches?				
	For Firewalls?				
	For IDS?				
	For RAS Systems?				
	For PBX Systems?				
Remarks:					
2.2.2	Is access to the AIS room restricted to personnel with a business need?				
	For Routers?				
	For Switches?				
	For Firewalls?				
	For IDS?				
	For RAS Systems?				
	For PBX Systems?				
Remarks:					
2.2.3	Is an inventory of the telecommunication system equipment maintained?				
	For Routers?				
	For Switches?				
	For Firewalls?				
	For IDS?				
	For RAS Systems?				
	For PBX Systems?				
Remarks:					

2.2.4	Is the inventory of telecommunication system equipment updated on a regular basis?				
	For Routers?				
	For Switches?				
	For Firewalls?				
	For IDS?				
	For RAS Systems?				
	For PBX Systems?				
Remarks:					
	Unused network ports should be turned off.	USDA DN/3040-6			
2.2.5	Are unused network ports turned off?				
	For Routers?				
	For Switches?				
	For Firewalls?				
	For IDS?				
	For RAS Systems?				
	For PBX Systems?				
Remarks:					

Period of: (Month/Year) _____ to (Month/Year) _____		
Reviewed by:	Name:	Signature:
Date Reviewed:		

2.3 ROUTERS

2.3.1 Identification and Authentication (I&A)

IDENTIFICATION AND AUTHENTICATION (I&A)					
Number	**Requirement**	**Source ***	**Y**	**N**	**N/A**
	Enable anti-spoofing via access lists on router.	BEST PRACTICES			
2.3.1.1	Verify that the border router is configured to have anti-spoofing enabled on interfaces.				
Remarks:					
	Strong password authentication is required.	USDA COMPTSR 11			
2.3.1.2	Verify that router exec mode password is set.				
Remarks:					
2.3.1.3	Verify that router privileged exec mode password is set.				
Remarks:					
2.3.1.4	Routers should follow USDA 3140-8 for password management.				
Remarks:					

2.3.2 Discretionary Access Control (DAC)

DISCRETIONARY ACCESS CONTROL (DAC)					
Number	**Requirement**	**Source ***	**Y**	**N**	**N/A**
	Examine SNMP access controls.	BEST PRACTICES			
2.3.2.1	Verify that SNMP default communications strings are changed from the default "public" and "private".				
Remarks:					
2.3.2.2	Verify that SNMP write access is disabled on routers that are externally accessible.				
Remarks:					
2.3.2.3	Verify the use of access control lists to control access to the SNMP functionality.				
Remarks:					

	Limit access to router.	BEST PRACTICES			
2.3.2.4	Is there an ACL that limits access to the router's virtual terminals?				
Remarks:					
2.3.2.5	Has a password been added to all inputs to the router (AUX, VTY, CON)?				
Remarks:					
2.3.2.6	Are the number of VTYs limited to the amount of administrators that may be required to use the router?				
Remarks:					
2.3.2.7	Is the "enable passwords" feature switched, to enable secret passwords?				
Remarks:					
	Display appropriate warning banners at login screen.	BEST PRACTICES			
2.3.2.8	Verify that "Message of the day" or login banner displays appropriate warning messages.				
Remarks:					
	Disable unnecessary services operating on routers.	BEST PRACTICES			
2.3.2.9	Verify that unnecessary services are disabled on any router that is reachable from a potentially hostile network. Examples: TCP & UDP, "Small Services", Finger.				
Remarks:					

2.3.3 Router IOS

ROUTER IOS					
Number	**Requirement**	**Source ***	**Y**	**N**	**N/A**
	The latest IOS with patches ensures the latest security features and fixes.	BEST PRACTICES			
2.3.3.1	Does the agency have a process for updating and applying the most recent maintenance releases to the IOS?				
Remarks:					
2.3.3.2	Is the IOS the most recent with all associated patches applied?				
Remarks:					
	Receiving the latest security information from the vendors is essential in maintaining security.	BEST PRACTICES			
2.3.3.3	Does the agency subscribe to a mailing list from the vendors for security problems?				
Remarks:					

2.3.4 Router Logging

ROUTER LOGGING					
Number	**Requirement**	**Source ***	**Y**	**N**	**N/A**
	Router should have external logging capabilities to a secure location.	BEST PRACTICES USDA COMPTSR 41			
2.3.4.1	Does the router send logs via syslog or SNMP trap logging to a secure host?				
Remarks:					
	Enable logging to all modes if required.	BEST PRACTICES			
2.3.4.2	If necessary, does the router log on all modes?				
Remarks:					
2.3.4.3	Are ACLs closed on the router?				
Remarks:					

Period of: (Month/Year) _____ to (Month/Year) _____		
Reviewed by:	Name:	Signature:
Date Reviewed:		

2.4 SWITCHES

2.4.1 Identification and Authentication (I&A)

IDENTIFICATION AND AUTHENTICATION (I&A)					
Number	**Requirement**	**Source ***	**Y**	**N**	**N/A**
	Strong password authentication is required.	USDA COMPTSR 11			
2.4.1.1	Verify that the switch exec mode password is set.				
Remarks:					
2.4.1.2	Verify that the switch privileged exec mode password is set.				
Remarks:					

2.4.2 Discretionary Access Control (DAC)

DISCRETIONARY ACCESS CONTROL (DAC)					
Number	**Requirement**	**Source ***	**Y**	**N**	**N/A**
	Limit access to the switch.	BEST PRACTICES			
2.4.2.1	Has the "enable passwords" feature been switched to use enable secret passwords?				
Remarks:					
2.4.2.2	Has a password been added to all inputs to the switch (AUX, VTY, CON)?				
Remarks:					
2.4.2.3	Are unused ports disabled?				
Remarks:					
2.4.2.4	Are the number of VTYs limited on the switch?				
Remarks:					
	Examine SNMP access controls.	BEST PRACTICES			
2.4.2.5	Verify that SNMP default communications strings are changed from the default "public" and "private".				
Remarks:					
2.4.2.6	Verify that SNMP "write" access is disabled on switches that are externally accessible.				
Remarks:					

2.4.2.7	Verify the use of access control lists to control access to the SNMP functionality.				
Remarks:					
	Warning banners should be displayed at login screen.	BEST PRACTICES			
2.4.2.8	Verify that "Message of the day" or login banner displays appropriate warning messages.				
Remarks:					

Period of: (Month/Year) _____ to (Month/Year) _____		
Reviewed by:	Name:	Signature:
Date Reviewed:		

2.5 FIREWALLS

2.5.1 Firewall Operating System

FIREWALL OPERATING SYSTEM					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	System on which the firewalls are installed should be secured in accordance to USDA requirements.	USDA COMPTSR			
2.5.1.1	Refer to checklist for operating system installation procedures.				
Remarks:					
	Only firewall services should be running on the platform.	BEST PRACTICES			
2.5.1.2	Does the firewall host have all services disabled except for those required to function?				
Remarks:					
	Maintaining an up-to-date OS is essential for firewall security.	BEST PRACTICES			
2.5.1.3	Are all relevant HotFixes or patches applied to the OS on which the firewall is based?				
Remarks:					
2.5.1.4	Has all the relevant maintenance been made to the firewall OS?				
Remarks:					

2.5.2 Firewall Management & Logging

FIREWALL MANAGEMENT & LOGGING					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	The system shall require users to identify themselves and provide some proof that they are who they say they are (e.g., user ID and password).	USDA COMPTSR 11			
2.5.2.1	Are remote management users authenticated in a secure fashion?				
Remarks:					
	Communications between the firewall and management console should be encrypted.	BEST PRACTICES			
2.5.2.2	If the management module is on a separate system, is the connection encrypted?				
Remarks:					

	Communication should use approved cryptology.	BEST PRACTICES			
2.5.2.3	Does the management station use approved cryptology to protect communications?				
Remarks:					
	Make sure that only legal and secure copies of the firewall software are being utilized.	BEST PRACTICES			
2.5.2.4	Are vendor-supplied licensed copies of the firewall software being used?				
Remarks:					
	Use the latest firewall software to insure the most up-to-date protection from security flaws within the application	BEST PRACTICES			
2.5.2.5	Does the management station have a process for updating and applying maintenance releases to the firewall?				
Remarks:					
	Use of full firewall capabilities provides for the best defense.	BEST PRACTICES			
2.5.2.6	Are the firewalls using all available security features, as appropriate?				
Remarks:					
	Logs should be monitored and analyzed for trends.	BEST PRACTICES			
2.5.2.7	Are the firewall logs checked on a daily basis in accordance with USDA 3140-6?				
Remarks:					
	Firewall systems should be able to alert the appropriate personnel of critical alerts on a timely basis.	BEST PRACTICES			
2.5.2.8	Are firewall alerting features used to send email or other communications to the appropriate security managers?				
Remarks:					
	Firewalls should be configured to be in a deny posture.	BEST PRACTICES			
2.5.2.9	Are the firewalls configured in “deny posture” in accordance with USDA 3140-6?				
Remarks:					

2.5.3 Firewall Rules

FIREWALL RULES					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	Only allow the minimal of services required to fulfill the mission.	USDA 3140-6			
2.5.3.1	Is the firewall rule set routinely reviewed to ensure that the rule set is kept to a minimum?				
Remarks:					
	Rules should also be reviewed for security.	USDA 3140-6			
2.5.3.2	Are rules routinely reviewed for optimal security?				
Remarks:					
	Keeping a backup enables a quick recovery from firewall failures/corruption.	BEST PRACTICES			
2.5.3.3	Is the rule-based backup in a secure location?				
Remarks:					

Period of: (Month/Year) _____ to (Month/Year) _____		
Reviewed by:	Name:	Signature:
Date Reviewed:		

2.6 IDS

2.6.1 IDS Operating System

IDS OPERATING SYSTEM					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	System on which the IDS is installed should be secured in accordance to USDA requirements.	USDA COMPTSR			
2.6.1.1	Refer to checklist for operating system installation procedures.				
Remarks:					
	Maintaining an up-to-date OS is essential for IDS security.	BEST PRACTICES			
2.6.1.2	Are all relevant HotFixes or patches applied to the OS on which the IDS is based?				
Remarks:					

2.6.2 IDS Management & Logging

MANAGEMENT & LOGGING					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	Using the latest IDS software ensures the most up-to-date protection from security flaws within the application.	BEST PRACTICES			
2.6.2.1	Is the latest version of the IDS software being used?				
Remarks:					
	The system shall require users to identify themselves and provide some proof that they are who they say they are (e.g., user ID and password).	USDA COMPTSR 11			
2.6.2.2	If the IDS is managed remotely, are there secure methods of authentication used to log on?				
Remarks:					
	Logs should be monitored and analyzed for trends.	BEST PRACTICES			
2.6.2.3	Are the IDS logs monitored on a daily basis in accordance with USDA 3140-6?				
Remarks:					
	IDS systems should be able to alert the appropriate personnel of critical alerts in a timely manner.	BEST PRACTICES			
2.6.2.4	Are the alerting capabilities being used?				
Remarks:					

2.6.3 IDS Policy

IDS POLICY					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	Maintain updated IDS signatures for the most up-to-date protection.	BEST PRACTICES			
2.6.3.1	Are the IDS signatures updated or reviewed at least weekly to reflect the changing threat environment?				
Remarks:					

Period of: (Month/Year) _____ to (Month/Year) _____		
Reviewed by:	Name:	Signature:
Date Reviewed:		

2.7 RAS SYSTEMS

2.7.1 Management & Logging

MANAGEMENT & LOGGING					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	All dial-up access to USDA's sensitive AIS and telecommunication networks shall be protected with devices or techniques that provide auditing.	USDA COMMSR 10 & 19 USDA COMPTSR 36			
2.7.1.1	Do the remote access system record alarms and authentication violations?				
Remarks:					
2.7.1.2	Is unauthorized activity reported?				
Remarks:					
	A waiver will be obtained for all entry points into the USDA network that do not pass through a firewall.	USDA 3140-6			
2.7.1.3	Has a waiver been obtained for all entry points into the USDA network that do not pass through a firewall?				
Remarks:					
2.7.1.4	Is the organization's internal network protected from the RSS?				
Remarks:					

2.7.2 Discretionary Access Controls

DISCRETIONARY ACCESS CONTROLS					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	The system will assure that users without authorization are not allowed access to the data.	USDA COMPTSR 9			
2.7.2.1	Do the remote access security controls protect audit records from unauthorized access?				
Remarks:					
2.7.2.2	Are banners displayed regarding unauthorized usage?				
Remarks:					
2.7.2.3	Are banners displayed regarding the usage and the monitoring policy?				
Remarks:					

	System information should be hidden.	BEST PRACTICES			
2.7.2.4	If system information is displayed before a successful logon, is the system-specific information masked (e.g. operating system version)?				
Remarks:					
	Dial-back authentication system should not be used as an alternative for user identification, authentication and audit trails.	USDA COMMSR 11			
2.7.2.5	Does the remote access system use a callback feature to enhance security?				
Remarks:					
2.7.2.6	Is the callback feature used as an alternative to a user ID?				
Remarks:					
	Modems should be secured and restricted.	BEST PRACTICES			
2.7.2.7	Are modem numbers unlisted from public sources?				
Remarks:					
2.7.2.8	Is dial-out allowed for organizations authorized modem usage?				
Remarks:					
2.7.2.9	Are methods used to identify unauthorized modems?				
Remarks:					
2.7.2.10	Is a modem pool used to limit modem usage?				
Remarks:					
2.7.3.11	Is an inventory kept of all modems?				
Remarks:					
2.7.3.12	Are modems allowed on user workstations?				
Remarks:					
2.7.3.13	Is there a policy in place to verify the need of a modem on a workstation?				
Remarks:					
2.7.3.14	Is the “dial-in” function disabled on workstation modems, if used?				
Remarks:					

2.7.3 Identification and Authentication (I&A)

IDENTIFICATION AND AUTHENTICATION					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	Documented process should exist to create and maintain user IDs for remote access users.	BEST PRACTICES			
2.7.3.1	Is there a process for authorizing new remote users?				
Remarks:					
2.7.3.2	Is there a documented process to maintain and verify access of user IDs on a regular basis?				
Remarks:					
	The system shall require users to identify themselves and provide some proof that they are who they say they are.	USDA COMPTSR 11 USDA COMMSR 10 & 12			
2.7.3.3	Do remote access security controls require that users be identified before access is granted?				
Remarks:					
2.7.3.4	Does each user have a unique user ID?				
Remarks:					
2.7.3.5	Are users allowed only one remote connection per user ID (or address), concurrently?				
Remarks:					
	Strong password management is required.	USDA COMPTSR 11 – 17 & 19 - 24			
2.7.3.6	Do the remote access systems store passwords in a one-way encrypted form?				
Remarks:					
2.7.3.7	Are remote access users required to change their passwords on a regular basis? (e.g. every 60 days)				
Remarks:					
	Passwords and user IDs should be immediately removed when an authorized user no longer needs access to the system.	USDA COMPTSR 18			
2.7.3.8	Is there a process to ensure user IDs and password are removed immediately as soon as an authorized user no longer needs access to the system?				
Remarks:					

Period of: (Month/Year) _____ to (Month/Year) _____		
Reviewed by:	Name:	Signature:
Date Reviewed:		

2.8 PBX SYSTEMS/KEY SYSTEMS

2.8.1 Protection Management

PROTECTION MANAGEMENT					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	Designated authority must maintain PBX equipment.	USDA A/MSR 22, 23			
2.8.1.1	Is there a particular person/group responsible for maintaining the equipment?				
Remarks:					
	Management must be briefed yearly on PBX-related issues.	USDA A/MSR 79			
2.8.1.2	Are top management briefed at least once a year about PBX issues such as protection issues, detected fraud levels, current protection etc.?				
Remarks:					

2.8.2 Protection Policy

PROTECTION POLICY					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	Written policy on phone and PBX use should be available.	USDA A/MSR 27; BEST PRACTICES			
2.8.2.1	Is there a written PBX policy available?				
Remarks:					
	The PBX policy is agreed to and signed by all employees and others with access to the facilities.	USDA A/MSR 85			
2.8.2.2	Has the PBX policy been read and signed by all employees and those with access to the facilities?				
Remarks:					
	The PBX policy includes specific guidelines on acceptable and unacceptable use of telecommunications within the organization, and specifies how uses explicitly not covered by the policy are dealt with.	BEST PRACTICES, USDA A/MSR 87			
2.8.2.3	Does the PBX policy include specific guidelines on acceptable usage of telecommunications within the organization?				
Remarks:					

2.8.3 Standards and Procedures

STANDARDS AND PROCEDURES					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	Telecom management at least once per month reviews PBX traffic, performance, circuit outage, and problem reports.	USDA A/MSR 65			
2.8.3.1	Are PBX related statistics and reports reviewed by telecom management on a monthly basis?				
Remarks:					
	Assure that only authorized personnel are allowed to request service level changes and/or report errors to the LEC, IXC and equipment vendors.	USDA PERSR 11; BEST PRACTICES			
2.8.3.2	Are only authorized personnel allowed to make service level changes?				
Remarks:					
	There is a periodic dump of all PBX parameters, which is automatically compared to the previous dump with differences reported to management.	BEST PRACTICES			
2.8.3.3	Are periodic dumps of all PBX parameters compared to the old dumps for discrepancies?				
Remarks:					
	Specific procedures should exist in order to make configuration changes to PBX software and hardware.	BEST PRACTICES			
2.8.3.4	Do specific procedures exist for configuration changes?				
Remarks:					
	PBX is backed up at least once a month.	USDA COMPTSR 41			
2.8.3.5	Are backups completed once a month?				
Remarks:					
	PBX backups should be stored off-site.	USDA COMPTSR 41			
2.8.3.6	Are backups stored off-site?				
Remarks:					
	Provide specific and identified standards and procedures for assuring the integrity, availability, and confidentiality of PBX operations.	BEST PRACTICES			
2.8.3.7	Are there specific procedures for assuring the integrity, availability and confidentiality of PBX operations?				
Remarks:					

2.8.4 Identification and Authentication (I&A)

IDENTIFICATION AND AUTHENTICATION					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	There is a process to create and maintain user IDs for the PBX system.	BEST PRACTICES			
2.8.4.1	Is there a process for authorizing new PBX users?				
Remarks:					
2.8.4.2.	Is there a process to maintain and verify access of user IDs on a regular basis?				
Remarks:					
	The system shall require users to identify themselves and provide some proof that they are who they say they are.	USDA COMPTSR 11 USDA COMMSR 10 & 12			
2.8.4.3	Do access security controls require that PBX users are identified before any requested actions are initiated?				
Remarks:					
2.8.4.4	Does each PBX user have a unique user ID?				
Remarks:					

2.8.5 Voice Mail – Special Features

VOICE MAIL – SPECIAL FEATURES					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	Voice mail and other PBX special feature assignments are controlled and documented.	USDA A/MSR 99; OMB-130, Appendix 3 BEST PRACTICES			
2.8.5.1	Are all voice mail configurations documented?				
Remarks:					
2.8.5.2	Does the system support more than one level of voice mail service?				
Remarks:					
2.8.5.3	Does the activation of voice mail service require management approval?				
Remarks:					

2.8.5.4	Has a risk assessment been performed for the voice mail system within the last three years?			
Remarks:				
2.8.5.5	Are all administrative functions performed on the voice mail system executed through dedicated or maintenance ports?			
Remarks:				
2.8.5.6	Are remote procedural commands for the voice mail system using dial-in enabled?			
Remarks:				
2.8.5.7	Are audit trails maintained for all voice mail administrative commands and configuration changes?			
Remarks:				
2.8.5.8	Is secondary dial tone disabled for all users?			
Remarks:				
2.8.5.9	If secondary dial tone is enabled, describe how it is controlled.			
Remarks:				
	Strong password management is required.	USDA COMPTSR 11 – 17 & 19 - 24		
2.8.5.10	Does the system enforce a minimal password length? (6 or more characters)			
Remarks:				
2.8.5.11	Are voice mail users required to change their passwords on a regular basis? (e.g. every 60 days)			
Remarks:				
	Passwords and user IDs should be immediately removed when an authorized user no longer needs access to the system.	USDA COMPTSR 18		
2.8.5.12	What is the time frame from when an individual leaves the organization to when the voice mailbox is disabled?			
Remarks:				

2.8.6 Documentation

DOCUMENTATION					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	A list of authorized point-of-contacts for all PBX-related issues, is maintained.	USDA A/MSR 99; BEST PRACTICES			
2.8.6.1	Is there a list of authorized contact points?				
Remarks:					
	Documentation such as network maps, topology diagrams, records, and policy statements should be readily available to all those responsible for PBX maintenance.	BEST PRACTICES			
2.8.6.2	Is all documentation readily available for authorized personnel?				
Remarks:					
	Circuit numbers are clearly marked on channel banks, CSU/DSUs, and modems.	BEST PRACTICES			
2.8.6.3	Are all the organization's channel banks, CSU/DSUs, and modems clearly marked with circuit numbers?				
Remarks:					

2.8.7 Technical Safeguards

TECHNICAL SAFEGUARDS					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	Direct inward system access capabilities are deactivated or removed from the PBX software.	USDA COMMSR 17; BEST PRACTICES			
2.8.7.1	Is all direct inward system access capabilities deactivated from the PBX software?				
Remarks:					
	Limit programming ports to specific ports in trusted areas.	BEST PRACTICES			
2.8.7.2.	Are all programming ports limited to trusted areas?				
Remarks:					
	Modems used for remote access to programming and/or maintenance ports are powered off except during periods when remote maintenance is being performed.	USDA COMMSR 22			
2.8.7.3	Are modems for remote access powered off, except during maintenance?				
Remarks:					

	An uninterruptible power supply is used to assure continuity of operation.	BEST PRACTICES			
2.8.7.4	Is there an uninterruptible power supply?				
Remarks:					
	The UPS is tested periodically to assure its proper operation.	BEST PRACTICES			
2.8.7.5	Is the UPS tested periodically?				
Remarks:					
	A generator is used to assure continuity of operation during sustained power outages.	BEST PRACTICES			
2.8.7.6	Is a generator used to assure continuity of operation in case of power outages?				
Remarks:					
	Administrative functions should only be performed from dedicated ports	BEST PRACTICES			
2.8.7.7	Are administrative functions performed on terminals that are connected to the PBX via the same type of ports, (switched between voice and data traffic), or are the terminals are connected via dedicated ports?				
Remarks:					

Period of: (Month/Year) _____ to (Month/Year) _____		
Reviewed by:	Name:	Signature:
Date Reviewed:		

2.9 CSU/DSU

2.9.1 General Security Items

Management					
Number	**Requirement**	**Source**	**Y**	**N**	**N/A**
	Circuit numbers are clearly marked on channel banks, CSU/DSUs, and modems.	BEST PRACTICES			
2.9.1.1	Are all the organization's channel banks, CSU/DSUs, and modems clearly marked with circuit numbers?				
Remarks:					
	Strong password authentication is required.	USDA COMPTSR 11			
2.9.1.2	CSU/DSUs should follow USDA 3140-8 for password management.				
Remarks:					

2.9.2 Discretionary Access Control (DAC)

ACCESS CONTROL (AC)					
Number	**Requirement**	**Source ***	**Y**	**N**	**N/A**
	Examine SNMP access controls.	BEST PRACTICES			
2.9.2.1	Verify that SNMP default communications strings are changed from the default "public" and "private".				
Remarks:					
2.9.2.2	Verify that SNMP write access is disabled on routers that are externally accessible.				
Remarks:					
2.9.2.3	Has a password been added to all inputs to the CSU/DSUs (AUX, VTY, CON)?				
Remarks:					
	Display appropriate warning banners at login screen.	BEST PRACTICES			
2.9.2.4	Verify that "Message of the day" or login banner displays appropriate warning messages.				
Remarks:					

2.9.3 CSU/DSU Firmware

ROUTER IOS					
Number	**Requirement**	**Source ***	**Y**	**N**	**N/A**
	The latest Firmware with patches ensures the latest security features and fixes.	BEST PRACTICES			
2.9.3.1	Does the agency have a process for updating and applying the most recent maintenance releases to the Firmware?				
Remarks:					
2.9.3.2	Is the Firmware the most recent with all associated patches applied?				
Remarks:					
	Receiving the latest security information from the vendors is essential in maintaining security.	BEST PRACTICES			
2.9.3.3	Does the agency subscribe to a mailing list from the vendors for security problems?				
Remarks:					

2.9.4 CSU/DSU Logging

ROUTER LOGGING					
Number	**Requirement**	**Source ***	**Y**	**N**	**N/A**
	CSU/DSU should have external logging capabilities to a secure location.	BEST PRACTICES USDA COMPTSR 41			
2.9.4.1	Does the CSU/DSU send logs via syslog or SNMP trap logging to a secure host?				
Remarks:					

Period of: (Month/Year) _____ to (Month/Year) _____		
Reviewed by:	Name:	Signature:
Date Reviewed:		

APPENDIX A - USDA REQUIREMENTS DOCUMENT

Administrative/Management Security Requirements

Requirement No	Requirement	Allocated
1	All USDA agencies and offices shall be in compliance with USDA security policies and procedures to include physical security, personnel security, telecommunications and information systems security, and emergency preparedness.	Facility
2	The Office of Chief Information Officer (OCIO) and the agencies shall assure the objectives of OMB Circular A-130 (Appendix III) are being met by establishing the minimum security requirements and guidelines to appropriately implement personnel security, physical security, industrial security, automated information system security, telecommunications security, operations security, and compliance.	Facility
3	The OCIO and agencies shall maintain inventories of sensitive applications and facilities (operational and under development) by name and brief description.	Facility
4	All existing USDA systems shall be in compliance with the USDA Information Systems Security Policy (ISSP), DR 3140-001.	Bureau or Agency
5	Requests for exceptions to USDA security requirements must include sufficient information to allow for a reasoned decision.	Bureau or Agency
6	Permanent exemptions from the requirement to clear residual data will be based on a risk analysis to determine what damage, if any, is caused by the potential disclosure of sensitive information to a user who does not have the same authorization to use some or all of the sensitive information on the automated information systems (AIS) network.	A
7	No exemption to object reuse is required for stand-alone AIS when all users are authorized access to all the sensitive information on the AIS.	A
8	A completed risk analysis shall accompany all requests for exceptions on existing dial-up circuits accessing sensitive AIS or networks. Time schedules will be included indicating when access control protection will be implemented on the dial-up circuits.	Bureau or Agency

9	A written exception to the Senior Information Resource Management Officer (SIRMO) shall be submitted for all facilities that cannot meet the baseline physical security requirements.	Facility
10	A full-time USDA Departmental ISSPM with appropriate authority and responsibility to manage the sensitive AIS and network security program for the USDA shall be designated.	Facility
11	The Departmental ISSPM shall establish a formal memorandum of understanding (MOU) among external agencies' accrediting authorities preceding telecommunication interconnections of accredited AIS.	Bureau or Agency
12	The Departmental ISSPM shall establish agency AIS and network programs.	Facility
13	The appointed Agency ISSPM shall determine the sensitivity of their information.	Bureau or Agency
14	The appointed Agency ISSPM will decide on the minimum safeguards prescribed for an AIS or network.	AIS
15	The appointed Agency ISSPM will execute a statement that an AIS or network is accredited.	AIS
16	The appointed Agency ISSPM will ensure that risk analysis responsibilities are accomplished in accordance with requirements.	Bureau or Agency
17	Management control systems must be established to document the requirements for each major information system and allow for periodic review of those requirements over the system's life.	Facility
18	Management control processes shall be established to assure that appropriate administrative, physical, and technical safeguards are incorporated into new applications, and into significant modifications to existing applications.	Facility
19	The management control process for applications considered sensitive shall include security specifications, design reviews, and system tests.	Facility
20	Procedures shall be established for periodically reviewing the continued need for, and manner of dissemination of, the agency information products or services.	Facility
21	Multi-year strategic planning processes shall be established for acquiring and operating information technology.	Facility
22	Responsibility for the security of each installation operated by or on behalf of the Federal Government shall be assigned to a management official knowledgeable in information technology and security matters.	Facility

23	The official whose program an information system supports shall be responsible and accountable for the products of that system.	Facility
24	An AIS security program shall be implemented and maintained.	Facility
25	A level of security shall be established for all agency information systems commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the information system.	Facility
26	All AIS facilities shall ensure that legal agreements with vendors include provisions for security (security clearances, where necessary, conflict of interest agreements, bonding of employees, nondisclosure agreements, personnel security screening, agreements establishing liability).	Facility
27	A clear desk policy should be established and enforced.	Facility
28	A Management Control Plan which identifies: component inventory risk ratings (high, medium, low), material weaknesses, and other areas of management concern must be developed and updated annually.	Facility
29	Each AIS or network being developed for operation beyond the year 2000 must be designed to meet the appropriate level of trust at which it is to be accredited.	Facility
30	The Departmental and Agency ISSPMs are required to thoroughly review all vendor recommendations and requirements for the configuration of security controls and formally document compliance or non-compliance of such requirements.	Bureau or Agency
31	Sensitive information shall be protected at a level commensurate with the threat. The level of protection will be determined by the criticality and sensitivity of the information and the mission supported by the system and in compliance with national policy and standards.	AIS
32	Telecommunications and information systems transmitting sensitive information should incorporate approved protection techniques consistent with applicable ISSP policies in the most cost-effective manner.	AIS
33	The minimum systems security standards for telecommunications and computer systems which process, store, transfer, or communicate sensitive information with an identified threat other than foreign, e.g., criminal, shall be compliance with the Federal Information Processing Standards (FIPS).	Bureau or Agency

34	An annual internal control report shall be provided to the President and the Congress that shall describe any security or other control weaknesses identified and provide assurance that there is adequate security of AISs.	Facility
35	A program should be established to conduct periodic risk analyses on AIS to determine if security baselines are met and to ensure that appropriate, cost-effective safeguards are incorporated on all new and existing AIS, networks, and facilities.	Bureau or Agency
36	Threat assessments shall be conducted at least every five years to ensure appropriate protection is implemented on critical and sensitive agency AIS and telecommunications systems.	AIS
37	A risk analysis shall be performed prior to the approval of design specifications for new installations.	AIS
38	A risk analysis must be performed to determine the need and type of approved protection techniques for critical or sensitive systems.	AIS
39	A risk analysis must be performed at periodic intervals established by the agency commensurate with the sensitivity of the data processed, but not to exceed every five years if no risk analysis has been performed during that period.	AIS
40	A risk analysis shall be performed whenever there is a significant change to the installation. A significant modification made to a sensitive AIS or network should require a review to determine the impact on the security of the processed sensitive information.	AIS
41	A risk analysis shall be performed for AIS processing sensitive information.	AIS
42	Risk assessments of Agency's AIS and telecommunications switch facilities shall be conducted to determine the types of threat and the appropriate physical protection measures.	Facility
43	Upon completion of system tests, a Certifying Official (Agency ISSPM) shall certify that the system meets all applicable Federal policies, regulations, and standards, and that the results of the tests demonstrate that the installed security safeguards are adequate for the application.	AIS
44	All new or major upgrades of existing critical, sensitive, or foreign intelligence AIS and networks shall be formally certified through a comprehensive evaluation of the technical and non-technical security features.	AIS
45	The certification, made as part of and in support of the accreditation process, shall determine the extent to which a particular design and implementation meets a specified set of security requirements.	AIS

	of security requirements.	
46	An official written declaration by an Agency ISPPM shall be issued for all certified AISs and networks to operate with specified security safeguards.	AIS
47	USDA information systems that process critical or sensitive, or foreign intelligence information will be certified and accredited by officially designated Agency ISSPMs.	AIS
48	Security testing shall be accomplished for certification purposes after installation of a product.	AIS
49	Pending accreditation, an interim approval to operate is permitted only if a security survey has been completed; a security plan has been developed to prevent unauthorized disclosure of data; a schedule describing advancement to the final accreditation must be established; and for systems processing TOP SECRET and foreign intelligence information, appropriate components must be located in properly secured facilities.	AIS
50	Interim approval to operate must be employed when a new system is in an advanced test phase and must use some actual operational data for final design and test before initial operational capability.	AIS
51	Evaluations of the technical and non-technical security features of the AIS and other safeguards shall be performed in support of the accreditation process.	AIS
52	Evaluations of the technical and non-technical security features of the networks and other safeguards shall be performed in support of the accreditation process.	AIS
53	Appropriate technical, administrative, physical, and personnel security requirements must be included in specifications for the acquisition or operation of information technology installations, equipment, software, and related services and shall be reviewed and approved by the management official responsible for security at the installation making the acquisition.	Bureau or Agency
54	Agency Administrators and ISSPMs shall ensure that all new information systems that store, process, or communicate sensitive information have security features incorporated during the conceptual design phase.	AIS
55	Agency Administrators and ISSPMs shall ensure that all new AISs that are intended to process, store, or communicate sensitive information incorporate the provisions of DM 3140-1 during the conceptual design phase.	AIS

56	All new telecommunications and AIS that store, process, transfer, or communicate critical, sensitive or foreign intelligence information shall have systems security features incorporated therein during the conceptual design phase.	AIS
57	All new telecommunications systems which communicate critical or sensitive information shall incorporate approved protection techniques during the planning stages and identify requirements in the five-year information system plans.	AIS
58	All new AIS or networks that are intended to process, store, or communicate sensitive information shall incorporate the provisions of this policy during the conceptual design phase.	AIS
59	The Departmental ISSPM shall periodically review all USDA information systems to ensure that provisions of the USDA ISSP are accomplished and provide a consolidated report to the Inspector General.	Facility
60	The System Security Manager Major Applications and Facility ISSPMs shall define and approve security requirements and specifications prior to acquiring or starting formal development of an AIS application.	Bureau or Agency
61	Security requirements and specifications shall be defined and approved prior to acquiring or starting formal development of applications.	AIS
62	Design reviews and system tests shall be conducted and approved prior to placing the application into operation.	AIS
63	Results of the design reviews and system tests shall be fully documented and maintained in the official agency records.	AIS
64	Acquisition specialists shall conduct and approve system design reviews prior to placing the system into operation to ensure the proposed design meets the approved security specifications.	AIS
65	The results of the system tests shall be fully documented and maintained in the official records.	AIS
66	Policies must be established and responsibilities assigned to assure that appropriate contingency plans are developed and maintained by end users of information technology applications.	AIS
67	Disaster recovery and continuity of operation plans for all information technology installations shall be maintained.	Facility
68	For large installations or installations that support essential agency applications shall develop and test disaster recovery plans and continuity of operations plans.	Facility

69	Essential emergency functions shall be performed at the headquarters and regional levels to maintain continuity of government during national security emergencies.	Facility
70	Vital records shall be identified in accordance with DR 3090-001.	Facility
71	The emergency operating records at storage locations for which the Vital Records Officer is accountable will be periodically inspected and certified for the currency and adequacy of the inventory following each inspection.	Facility
72	Assembling, packing, and arranging for shipment of the vital records to appropriate storage locations shall be assured.	Facility
73	OMB Circular A-130 requires appropriate contingency, disaster, and continuity planning for AIS applications and their implementation (facilities). The plans shall be tested periodically for their adequacy and effectiveness.	Bureau or Agency
74	A disaster recovery and contingency plans shall be developed for AISs processing sensitive information..	AIS
75	A security awareness and training program shall be established.	Bureau or Agency
76	The Departmental ISSPM and Agency ISSPMs as it relates to their respective agencies and offices, develop, maintain, and update annually security awareness and training plans and reports in accordance with the guidelines attached to this directive.	Facility
77	Training and awareness plans shall be developed, maintained, and updated annually by USDA agencies. Plans must contain, at a minimum, the following information: (a) training content or subject matter; (b) target audience, including bureau and contractor personnel for each of the training content areas; and {c} level of training to be provided for each specific subject matter area and target audience category.	Facility
78	USDA personnel, including contractors, who are involved with the management, use, or operation of any telecommunications or AIS handling sensitive or critical information within or under the supervision of the Department, shall receive periodic training in security awareness and accepted security practices.	Facility
79	All personnel shall receive an annual threat briefing.	Facility
80	Current telecommunications and AIS threat and vulnerability briefings shall be provided to USDA agencies and offices.	Facility

81	For users of systems which process, store, or communicate sensitive information, initial training shall be provided as soon as possible and within a minimum of 60 days of appointment for new personnel who are managers, users, or operators of sensitive information systems.	Facility
82	For users of systems which process, store, or communicate sensitive information, continuing training shall be provided whenever there is significant change in the telecommunications and AIS environment or procedures.	AIS
83	For users of systems which process, store, or communicate sensitive information, refresher training shall be provided on an annual basis for all personnel responsible for the management, use or operation of sensitive information system.	Facility
84	AIS and network users shall have an initial security briefing meeting. The initial briefing will be acknowledged in writing. Thereafter, periodic, though at least annual, refresher training will be provided to each group of users.	Facility
85	All personnel who install, operate, maintain, or use the AIS have been authorized access to use the AIS, shall be familiar with documented security practices before gaining access to the AIS, and be acknowledged in writing applicable system security requirements and responsibilities.	Facility
86	Appropriate administrative, technical, and physical safeguards shall be established to insure the security and confidentiality of records containing Privacy Act Information.	Facility
87	Policies and practices regarding the storage, retrievability, access controls, retention, and disposal of Privacy Act Information shall be established.	Facility
88	Each agency that maintains a system of records shall promulgate rules which shall establish procedures for the disclosure to an individual upon his request of his record.	Facility
89	Individuals shall be provided with access to, and the ability to amend errors in, systems of records consistent with the Privacy Act, Section 552a.d.	Facility
90	Data shall be recorded and reported to provide users of the data with complete information about the subject of the report per OMB, USDA, and Privacy Act standards.	Bureau or Agency
91	A five-year plan for a single integrated, efficient agency financial management system shall be developed.	Facility
92	Financial management data (for financial management systems) shall be gathered and processed only where necessary to meet specific internal management needs or external requirements.	AIS

	external requirements.	
93	Financial management data (for financial management systems) shall be recorded as soon as practicable after the occurrence of the event.	AIS
94	Financial management information (from financial management systems) shall be recorded and reported in the same manner throughout the agency, using uniform definitions.	AIS
95	Financial management systems shall be designed and operated with reasonable total costs and transaction costs, in accordance with OMB guidelines.	AIS
96	A plan for the security and privacy of each Federal computer system identified by that agency shall be established that is commensurate with the risk and magnitude or the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system.	AIS
97	Security plans shall be reviewed annually.	AIS
98	The Senior Information Resource Management Officer (SIRMO) shall appoint in writing a System Security Manager Major Applications for the AIS under their control.	Bureau or Agency
99	A memorandum with the appointed System Security Manager Major Applications name, work address, telephone number, and security clearance (if applicable) shall be developed.	Bureau or Agency
100	All USDA agencies shall establish a network security program ensuring all AISs and their supporting telecommunications are authorized, authenticated, protected, and accounted.	Bureau or Agency
101	The SIRMO shall appoint in writing a Network Security Officer (NSO) for the networks under their control.	Bureau or Agency
102	All agencies shall implement a program designed to minimize the risk of introducing viruses and other malicious software into critical, sensitive , or foreign intelligence AIS and networks.	Bureau or Agency
103	PC systems to which access is somewhat open, (i.e., training rooms, etc.) should never be used as a source of software or files to be transmitted and/or copied for distribution without first taking steps to ensure that the system is free from viruses or other malicious software.	Facility
104	A virus or other malicious software program shall be immediately reported to your supervisor and Agency ISSPM prior to being fixed.	Facility

105	An individual at any level of employment who is determined to have been responsible for the unauthorized release or disclosure, or potential release or disclosure, of classified information, either knowingly, willfully or through negligence, shall be notified that the action is in violation of applicable USDA regulation.(DM 3440-1.3)	Facility
106	Any security violation possibly involving an infraction of Federal criminal laws or a senior USDA official shall be forwarded by the designated Agency ISSPM, to the Departmental and Agency ISSPM and concurrently to the Inspector General.	Facility
107	USDA agencies shall submit annual "Agency Information Security Program Data" reports.	Facility
108	The Agency ISSPM shall maintain a record for not less than 12 months of all personnel requiring escorted access to the central computer facility, which has the visitor's name, organization, reason for the visit date and time of arrival and departure, and the escort's name and signature.	Facility
109	The SIRMO or Agency ISSPM will document the duties required to secure the AIS facility and the System Security Manager Major Applications will acknowledge these duties.	Bureau or Agency
110	The Agency ISSPM shall maintain a current access roster containing the name, organization, and access authorization of each individual requiring routine unescorted access to remote terminal areas.	Facility
111	The Agency ISSPM shall maintain a record for not less than 12 months of all personnel requiring escorted access to the remote terminal area, which has the visitor's name, organization, reason for the visit, date and time of arrival and departure, and the escort's name and signature.	Facility
112	Logs shall be required for recording all physical access to the facility by unauthorized individuals (i.e., vendor maintenance and local telephone company personnel, etc.).	Facility
113	Maintain and retain physical access (to the facility) logs for a minimum of two years.	Facility

Physical Security Requirements

Requirement No	Requirement	Allocation
1	Physical security for the central computer facility will be commensurate with, or exceed, the minimum requirements of the most restrictive category (or highest classification) of information that may be processed by the system.	Facility
2	If two or more separate systems are located within the confines of a single controlled access area, physical security and access control systems will be those appropriate for the most sensitive (or highest classified) data in either system.	Facility
3	During working hours, remote on-line terminals and terminal processing areas shall be secured commensurate with the most restrictive category (or highest classification) of data that the area has been approved to process.	Facility
4	During non-working hours, the terminal equipment and communication lines shall be protected so as to inhibit theft of Government property and to provide evidence of unauthorized entry.	Facility
5	Storage of classified information on AIS fixed hard disks, (i.e., personal computers, microcomputers, etc.) is only authorized when such equipment is contained within an open-storage facility approved for classified information.	Bureau or Agency
6	Sensitive information marked with an Agency legend shall be safeguarded in accordance with established agency standards.	Facility
7	All agencies shall adequately protect their facilities used to process, transmit, or store sensitive information in support of critical operations and missions.	Facility
8	The facility should be locked at all times when authorized personnel are not present. If undetected entry can occur while the facility is occupied, countermeasures shall be implemented to restrict unauthorized access.	Facility
9	Unescorted entry to either the central computer facility or a remote terminal area must be controlled and limited to personnel authorized to use the system.	Bureau or Agency
10	Personnel escorting personnel who are not authorized or approved for unescorted access into the central computer facility or remote terminal areas should be aware of their responsibilities.	Facility
11	Escorts shall be provided for unauthorized individuals at all times. Escorts will have authorization for access to all areas of the facility.	Facility

12	Computers and terminals should be locked or the keyboard disconnected and stored in a secure location, when not in use, to prevent unauthorized access. Lock doors to areas containing computers and terminals.	Facility
13	The entrance(s) doors to an AIS or telecommunications facility shall be solid wood or metal at least 1-3/4 inches thick.	Facility
14	Deadbolt locks with a one-inch throw and a high security cylinder (e.g., Medeco D-11 Series) shall be used to secure the facility doors.	Facility
15	Keys should never be left in locks or hidden in an area near the lock.	Facility
16	The distribution of keys should be strictly limited and an effective control system established. Keys should be "off master" in buildings shared with other entities.	Facility
17	During non-duty hours, the cipher lock should not be used as a sole locking device. Cipher locks should utilize a minimum of four numbers.	Facility
18	The cipher combination should be protected by shielding the locking mechanism against observation by unauthorized personnel.	Facility
19	Cipher locks shall have key overrides, and combinations shall be changed at least: once every six months; when anyone with the current combination resigns or transfers; or when an attempt to compromise the combination (either successful or unsuccessful) is made	Facility
20	Perimeter walls shall be slab to slab in construction and permanently attached to true floor and true ceiling.	Facility
21	Ground level and second story windows shall have positive locking devices installed.	Facility

Personnel Security Requirements

Requirement No	Requirement	Allocation
1	Personnel security policies and procedures shall be established and managed to assure an adequate level of security for Federal AISs.	Facility
2	The coding of position sensitivity is required on Optional Form 8, Position Description (or an equivalent agency form). Agencies must use the following codes when coding position sensitivity: Special Sensitive-4; Critical Sensitive-3; Non-critical Sensitive-2; Nonsensitive-1. Computer and ADP positions will also be identified by the letter "C" after the above code.	Facility
3	Individuals assigned to emergency management teams must possess the requisite security clearance: BRAVO team - final TOP SECRET clearance; ALPHA and CHARLIE teams - SECRET clearance.	Facility
4	Personnel having Military Ready Reserve assignments should not be assigned to emergency management teams.	Facility
5	Position sensitivity criteria, similar to what is applied to Federal personnel, must be applied to contractor relationships.	Facility
6	All positions that have national security duties must be designated at national security sensitivity levels. Levels include Special Sensitive, Critical Sensitive, and Non-critical Sensitive.	Facility
7	The individuals designated as representatives to the USDA Telecommunications and Information Systems Security Working Group should have or should be eligible for a SECRET clearance.	Facility
8	Required background investigations are required for placement at each of the sensitivity levels: Special Sensitive: Special Background Investigation; Critical Sensitive: Background Investigation (BI); Non-critical Sensitive: Limited BI or Minimum BI; Non-sensitive: National Agency Check and Inquiry (NAC&I).	Facility
9	The incumbent of each position designated Special Sensitive or Critical Sensitive shall be subject to periodic reinvestigation five years after placement, and at least once each succeeding five years.	Facility
10	Personnel applying for critical sensitive positions must undergo a pre-placement background investigation.	Facility
11	Only authorized personnel shall have access to information systems.	Bureau or Agency

12	Granting access to any classification level must be made on a need-to-know basis, and when that need no longer exists, access must be canceled.	Bureau or Agency
13	On-site personnel who operate ADP equipment shall be approved for access to all types of restricted access data contained in the system and instructed on appropriate security procedures before being granted unescorted system access.	Facility
14	Appropriate supervisors and security professionals shall be approved for access to all types of restricted access data contained in the system and instructed on appropriate security procedures before being granted unescorted system access.	Bureau or Agency
15	Personnel who design, develop, install, modify, service, or maintain the operating system software shall be approved for access to all types of restricted-access data contained in the system and instructed on appropriate security procedures before being granted unescorted access.	Bureau or Agency
16	Communication specialists who are responsible for maintenance of the communications hardware and software among ADP facilities or between an ADP facility and its remote terminal users and have the capacity to monitor unencrypted communications shall be approved for access to all types of restricted access data contained in the system and instructed on appropriate security procedures before being granted unescorted system access.	Bureau or Agency

Information Security Requirements

Requirement No	Requirement	Allocation
1	Agencies shall provide written identification of the definition of any respective legend(s) and establish protective requirements, as applicable, which shall be made known to all authorized recipients.	Facility
2	The legend "Limited Official Use" shall be marked, stamped, or permanently affixed to the top and bottom of the outside of the front and back covers, on the title page, on the first and last pages, and on all pages of documents or information requiring control.	Bureau or Agency
3	The identity of the official authorizing the use of the legend and the date of such authorization shall appear on the first and last pages of all LOU documents or information.	Bureau or Agency
4	Legends should be removed as soon as they are no longer needed.	Bureau or Agency
5	The identity of the official authorizing the decontrol of a document or information, as well as the date of such authorization, shall appear on the first and last pages of all decontrolled documents.	Bureau or Agency
6	Cover sheets must be used to protect the LOU information while in use.	Bureau or Agency
7	File folders containing LOU information shall be marked (e.g., at the top and bottom of the front and back covers).	Facility
8	A warning label shall be affixed to diskettes or floppy disks that contain LOU.	Bureau or Agency
9	Officials authorized to control and/or decontrol LOU information shall be listed by name and position title .	Facility
10	USDA officials responsible for responding to the request for release of LOU shall determine, under FOIA/Privacy Act criteria or the appropriate regulations of the USDA agency concerned, whether the information should be made available to the requestor.	Facility
11	Security standards equivalent to national security CONFIDENTIAL are required for information marked for LOU when the information is electronically processed, stored, transferred, or communicated.	Bureau or Agency
12	Safeguard LOU information in the same manner as national security information classified CONFIDENTIAL.	Bureau or Agency
13	LOU information shall be made available only to those persons having a need-to-know.	Bureau or Agency

14	LOU information or material shall NOT be hand-carried aboard commercial passenger aircraft by DO or agency officials unless the security representative authorized to direct official travel within their office or agency has made a prior written determination that an emergency situation exists.	Facility
15	LOU information or material shall normally be transmitted by one of the means established for higher classifications or by the U.S. Postal Service Express Mail or U.S. Postal Service registered first class mail.	Facility
16	Personnel designated as couriers shall have in their possession an employee ID card or credential with a photograph, descriptive data and bearer's signature.	Facility
17	Travelers shall NOT authorize the opening of carry-on items under any circumstance.	Facility
18	LOU documents being carried shall be in the form of paper documents with no metal bindings and contained in sealed opaque inner and outer envelopes.	Facility
19	Officials who authorize transportation of classified and LOU information material shall notify an official of the appropriate air carrier in advance.	Facility
20	Couriers shall have an original of a letter authorizing them to carry classified or LOU information or material.	Facility
21	All pages of a LOU transmittal document shall show the control designation of the information being transmitted.	Facility
22	The Departmental ISSPM shall ensure that procedures are developed to protect sensitive reports during preparation, transmittal, receipt and storage.	Facility
23	Copies of risk analysis shall be available to risk analysis teams, internal control personnel and the agency ISSPM on a need-to-know basis. Reports shall be kept in a secure area commensurate with the sensitivity of information contained in the report.	Bureau or Agency
24	A copy of all documentation relating to security violations shall be filed in the security violation indexes of the USDA Office of Inspector General, or the Agency ISSPM, and also in the individual's personnel security file.	Facility
25	Procedures will be in place to ensure the secure destruction of discarded computer material to preclude unauthorized disclosure.	Facility

Communications Security Requirements

Requirement No	Requirement	Allocation
1	Heads of agencies shall formally designate an individual to serve as the bureau COMSEC officer for reporting possible compromise or loss of COMSEC equipment and material.	Facility
2	Heads of agencies shall establish procedures to ensure that any possible compromise or loss of COMSEC equipment and material is reported to the Departmental ISSPM and to the appropriate Agency COMSEC officer to evaluate incidents and initiate actions to minimize impacts.	Facility
3	The Departmental and Agency ISSPMs shall certify and maintain a list of approved Electronic Funds Transfer (EFT) authentication equipment and software techniques.	Facility
4	The selection of off-the-shelf encryption equipment for communications security must be Federal Standard 1027 equipment or endorsed equipment from the commercial COMSEC Endorsement Program.	Facility
5	USDA Central Office of Record COMSEC accounts will ensure strict control over COMSEC material under their control.	Facility
6	All key material used for the protection of classified national security or sensitive information will be generated, distributed, stored, and destroyed in a secure and controlled manner.	Facility
7	Written guidelines shall be established in the form of a key management plan for the handling and safeguarding of keying material.	Facility
8	Sensitive information must be encrypted using either NSA Type 2 encryption, NSA endorsed Data Encryption Standard (DES), or DES devices determined to be compliant with the appropriate FIPS.	AIS
9	Unencrypted cable (guided media) may be used within the geographic boundaries of the U.S., Alaska, Hawaii, U.S. territories and possessions, and with adequate measures to discourage radio transmission.	AIS
10	All dial-up access to USDA's sensitive AIS and telecommunication networks shall be protected with Federal government approved devices or techniques that provide explicit user identification and authentication, and audit trails.	Bureau or Agency
11	A dial-back authentication system should not be used as an alternative for user identification, authentication, and audit trails.	Bureau or Agency

12	Access control in the form of well-administered user name and authentication shall be established for each user having dial-in access.	Bureau or Agency
13	The systems own journaling or logging capability should always be used to monitor all communications activity with the host, to determine system/network usage, identify user difficulties and uncover intrusion attempts.	Bureau or Agency
14	USDA-owned PBXs shall be provided minimum system and physical protection. This protection is required due to the increasing threat to digital telephone switches and digital key systems.	Bureau or Agency
15	New facilities which will process, store, or communicate critical or sensitive information shall incorporate telephone security during the planning stages.	Facility
16	Locks, access logs, and escort procedures are minimum requirements for the physical protection of digital switch and key system facilities.	Facility
17	Avoid co-locating the PBX system(s), voice mail system(s), and their administrative terminals with other equipment requiring human access.	Facility
18	Maintenance personnel shall be escorted by the Network Security Officer or a person with knowledge of the system.	Facility
19	An access log shall be maintained.	Facility
20	PBX system passwords should be changed semi-annually and be held only by the NSO or by a delegated authority. Passwords shall be set to the maximum length allowed by the system.	AIS
21	In instances where the vendor controls the remote maintenance password for the systems maintenance and remote maintenance access, request a copy of the vendor's policy regarding password administration.	AIS
22	The activation of the remote access feature should be avoided unless great care is taken to protect the system from unauthorized access. "Barrier Codes" must be used if this feature is activated. The codes will be set to the maximum length allowed by the PBX system.	Bureau or Agency

Computer Security Requirements

Requirement No	Requirement	Allocation
1	Personally-owned computers or software will not be used to process, access, or store sensitive information without the approval of the Agency ISSPM.	AIS
2	Configuration control plans shall be prepared and configuration management shall be implemented in all critical, sensitive and foreign intelligence AIS and networks.	AIS
3	Configuration control should begin in the earliest stages of the design and development of the system or network and extend over the full life of the configuration items included in the design and development stages.	AIS
4	For every change that is made to an AIS or network, the design and requirements of the changed version of the system should be identified.	AIS
5	Every change made to documentation, hardware, and software/firmware should be reviewed and approved by the Agency ISSPM, Network Security Officer, or the available security staff.	Bureau or Agency
6	Configuration status accounting is responsible for recording and reporting on the configuration of the project throughout the change.	AIS
7	Through the process of a configuration audit, the completed change can be verified to be functionally correct, and for trusted systems and networks, consistent with the security policy of the system or network.	AIS
8	In the case of a change to hardware or software/firmware that will be used at multiple sites, configuration control is also responsible for ensuring that each site receives the appropriate version of the system or network.	Bureau or Agency
9	The system will assure that users without authorization are not allowed access to the data.	AIS
10	System users shall be provided the capability to specify, at their discretion, who (by individual users or user, groups, etc.) may have access to their data.	AIS
11	The system shall require users to identify themselves and provide some proof that they are who they say they are (e.g., user ID and password).	AIS
12	A password should not be shared by multiple users.	AIS
13	The system should prevent a user from choosing a password that is already associated with another user ID.	AIS

14	The system should store passwords in a one-way encrypted form.	AIS
15	The system should automatically suppress or fully blot out the clear-text representation of the password on the data entry device.	AIS
16	The system should block any demonstration of password length (i.e., the cursor should not move upon input).	AIS
17	The system, by default, should not allow null passwords during normal operation.	AIS
18	Passwords and user IDs should be immediately removed when an authorized user no longer needs access to the system.	Bureau or Agency
19	The system should provide a mechanism to allow passwords to be user-changeable.	AIS
20	The system should enforce password aging on a per-user basis. The system-supplied default for all non-privileged users should be no more than 60 days and no more than 30 days for user IDs that may acquire privileges. After the password aging threshold has been reached, the password shall no longer be valid and should require action by the Agency ISSPM to reset the password.	Bureau or Agency
21	The system should provide a mechanism which notifies the user to change their password.	AIS
22	Passwords should not be reusable by the same individual for a period of time specified by the Agency ISSPM. The system-supplied default should be six months.	AIS
23	The system should provide a method of ensuring the complexity of user-entered passwords (e.g., eight characters minimum length).	AIS
24	As soon as the system has been installed, all vendor supplied passwords, including those for software packages and maintenance accounts should be changed.	AIS
25	Terminals, workstations and networked personal computers should never be left unattended when user ID and password have been logged in.	Bureau or Agency
26	AISs and networks which process, store, or transmit sensitive information shall meet the requirements for C2 level protection as evaluated by the National Security Agency or the National Institute for Standards and Technology.	AIS
27	If a network is accessed by a user who is not authorized to use all or some of the sensitive information processed by or communicated over the network (or if the network is accessed by dial-up circuits), C2 protection shall be implemented on microprocessors running UNIX or other multi-user, multi-tasking operating systems.	AIS

28	Until C2 products are available, interim discretionary access control protection measures for microcomputers shall be implemented.	AIS
29	As an interim measure, specialized automated techniques shall be used to verify the proper output classification of data until the incorporation of trusted products is feasible, or a new AIS can be designed and implemented to meet the specified level of trust.	AIS
30	When a storage object (e.g., core area, disk file, etc.) is initially assigned, allocated, or reallocated to a system user, the system shall assure that it has been cleared.	AIS
31	The system shall define and control access between named users and system resources (e.g., files and programs)	AIS
32	Sensitive AIS and networks shall be protected to at least the minimum level of controlled access protection (C2) .	AIS
33	The system must protect authentication data so that it may not be accessed by an unauthorized user.	AIS
34	The system shall be able to create, maintain, and protect from modification, unauthorized access, or destruction an audit trail of accesses to the resources it protects.	AIS
35	The audit data shall be protected by the system so that read access to it is limited to those who are authorized for audit data.	AIS
36	The system shall be able to record the following types of events: log on, log off, change of password, creation, deletion, opening, and closing of files, program initiation, and all actions by system operators, administrators, and security officers. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and the success or failure of the event.	AIS
37	For log on, log off, and password change the origin of the request (e.g., terminal ID) shall be included in the audit record. For file related events, the audit record shall include the file's name.	AIS
38	The Departmental and Agency ISSPMs shall be able to selectively audit the actions of one or more users based on individual identity.	Bureau or Agency
39	Audit procedures shall be developed and coordinated with other internal control procedures required under OMB Circular A-123.	Bureau or Agency
40	New software should be backed up immediately, retaining the original distribution diskettes in a safe and secure location. Write-protect original diskettes prior to making backup copies.	AIS
41	Data files should be backed up frequently and stored off-site or in a secured environment.	Bureau or Agency

42	Damaged software programs should be restored from the original diskettes, not from regular backups.	AIS
43	Use only new media for making copies for distribution.	AIS
44	PC machine-readable media should be scanned for malicious software before initial use. Write-protect software prior to scanning to prevent possible contamination from system and virus scan software being used.	Facility
45	Software obtained electronically from bulletin boards shall be downloaded to newly formatted diskettes and not directly to the computer hard disk.	Facility
46	PC hard disk drives, network file servers and other media which will be used to handle agency information should be formatted between the time they are received and put into use.	Facility
47	Never start up (boot-up) a computer from a diskette unless it is the original write-protected system master or a trusted copy.	Facility
48	Portable computer systems, such as laptops, that leave agency controlled areas shall be scanned for viruses before and after connecting to systems or software owned by other organizations.	Facility
49	The decision to safeguard sensitive storage media during its life cycle should be based on a risk analysis to access the threat to the sensitive information.	Bureau or Agency
50	A purge is not complete until a final overwrite is made using unclassified data.	AIS
51	Media should be purged before submitting it for destruction.	AIS
52	Degaussing with an approved degausser is the only method acceptable for purging classified or unclassified intelligence information media.	AIS
53	Overwrite software shall be protected at the level of the media it purges. The overwrite software must be protected from unauthorized modification.	AIS
54	Magnetic tape should have a label applied to the reel that identifies the coercivity of the media. Labels that show the classification should not be removed from the reel until the media is declassified.	Facility
55	Leased equipment containing non-removable magnetic storage media should not be returned to the vendor unless the media is declassified using an approved procedure.	Facility
56	Once sensitive information has been written to the hard-drive of a personally owned computer, the sensitive data shall be completely erased when it is no longer needed on the system to preclude disclosure or data corruption.	Bureau or Agency

57	Controls for local area networks shall be established that prevent anyone except authorized staff from loading software on file servers.	Facility
58	A local area network file server shall never be used as a workstation.	Facility
59	File servers shall be located in areas where access is restricted.	Facility
60	Security Features User's Guide: A single summary, chapter, or manual in user documentation shall describe the security features provided by the Trusted Computing Base, guidelines on their use and how they interact with one another.	AIS
61	A Trusted Facility Manual: A manual addressed to the ADP security administrator shall present cautions about functions and privileges that should be controlled when running a secure facility.	Facility
62	Test documentation: The system developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and results of the security mechanisms' functional testing.	AIS
63	Design documentation: Documentation shall be available that provides a description of the manufacturers philosophy of protection and an explanation of how this philosophy is translated into the Trusted Computing Base (TCB). If the TCB is composed of distinct modules, the interfaces between these modules shall be described.	AIS
64	The stand-alone hardware should be scanned before it is used by the vendor to verify that the computer does not contain any viruses.	Bureau or Agency
65	The stand-alone hardware should be scanned when the demonstration is completed to determine if the vendor software contains a virus and remove it from the system.	Bureau or Agency
66	Written certification from the vendor that the demonstration software has been checked and is free from viruses shall be obtained prior to loading any vendor software.	Bureau or Agency

APPENDIX B - ACRONYMS AND ABBREVIATIONS

AIS	Agency Information System
BEST PRACTICES	Industry Best Practices
CCB	Configuration Control Board
CSU/DSU	Channel Service Unit / Data Service Unit
DAC	Discretionary Access Control
I&A	Identification and Authentication
IDS	Intrusion Detection System
IOS	Internetwork Operating System
ISSPM	Information Systems Security Program Manager
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OS	Operating System
PBX	Private Branch Exchange
PDD	Presidential Decision Directive
RAS	Remote Access System
SNMP	Simple Network Management Protocol
UPS	Uninterruptible power supply
USDA A/MSR	Administrative/Management Security Requirements
USDA COMMSR	Communications Security Requirements
USDA COMPTSR	Computer Security Requirements
USDA ISR	Information Security Requirements
USDA PERSR	Personnel Security Requirements
USDA PHYSR	Physical Security Requirements
USDA	United States Department of Agriculture